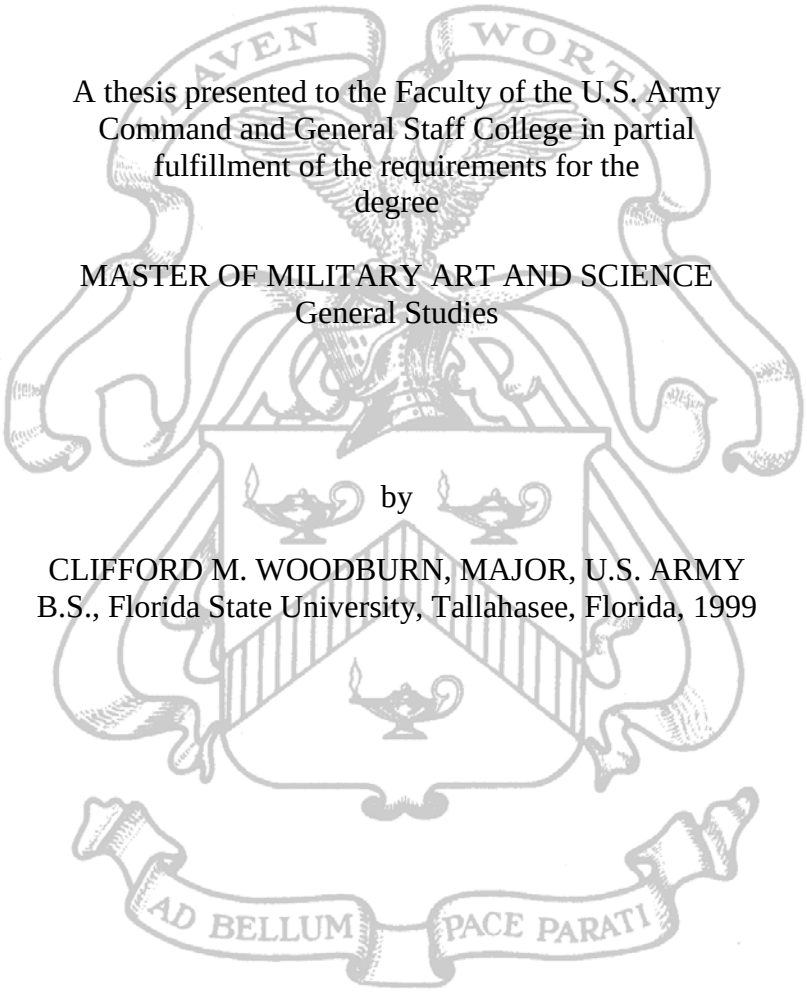
LEADER DEVELOPMENT OF CYBER SOLDIERS THROUGH MISSION COMMAND

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

CLIFFORD M. WOODBURN, MAJOR, U.S. ARMY
B.S., Florida State University, Tallahasee, Florida, 1999



Fort Leavenworth, Kansas
2013-01

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
14-06-2013	Master's Thesis	AUG 2012 – JUN 2013

4. TITLE AND SUBTITLE

Leader Development of Cyber Soldiers through Mission Command

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Major Clifford M. Woodburn, U.S. Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Technology and the digital environment have introduced and influenced one of the most dynamic and asymmetric battlefields of the 21st century. The vulnerability of ever expanding Department of Defense digital resources has led to increased concerns over the segregation of these resources across the government. The ever growing joint and inter-agency operational environment will mold cyber warriors, and shift the dynamics of how to develop cyber leaders. Commanders must develop dynamic, knowledgeable leaders to combat the emerging cyber threats, while establishing learning environments that allow for disciplined initiative. Futhermore, organizations must have an established culture that fosters prudent risk, while ensuring that failure in the system is survivable. Lastly, organizations must learn from their failures, by converting lessons observed into lessons learned. Due to the demands of cyberspace, a cyber warrior must be agile, adaptive, and technically and tactically proficient in defending the network. The direct correlation between Mission Command and cyber leader development was inconclusive due to the number of variables, though the research proved elements of Mission Command are guiding potential development of cyber leaders.

15. SUBJECT TERMS

Cyberspace, Leader Development, Mission Command

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	76	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Major Clifford M. Woodburn, U.S. Army

Thesis Title: Leader Development of Cyber Soldiers through Mission Command

Approved by:

_____, Thesis Committee Chair
LTC Tacildayus Andrews, MMAS

_____, Member
Nellie Goepferich, Ph.D.

_____, Member
LTC Frank Snyder, M.S.

Accepted this 14th day of June 2012 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

LEADER DEVELOPMENT OF CYBER SOLDIERS THROUGH MISSION COMMAND, by Major Clifford M. Woodburn, U.S. Army, 76 pages.

Technology and the digital environment have introduced and influenced one of the most dynamic and asymmetric battlefields of the 21st century. The vulnerability of ever expanding Department of Defense digital resources has led to increased concerns over the segregation of these resources across the government. The ever growing joint and inter-agency operational environment will mold cyber warriors, and shift the dynamics of how to develop cyber leaders. Commanders must develop dynamic, knowledgeable leaders to combat the emerging cyber threats, while establishing learning environments that allow for disciplined initiative. Futhermore, organizations must have an established culture that fosters prudent risk, while ensuring that failure in the system is survivable. Lastly, organizations must learn from their failures, by converting lessons observed into lessons learned. Due to the demands of cyberspace, a cyber warrior must be agile, adaptive, and technically and tactically proficient in defending the network. The direct correlation between Mission Command and cyber leader development was inconclusive due to the number of variables, though the research proved elements of Mission Command are guiding potential development of cyber leaders.

ACKNOWLEDGMENTS

I would like to express my sincere appreciation to my research committee, LTC Tacildayus Andrews, Dr. Nellie Goepferich, and LTC Frank Snyder, for their guidance and support throughout the course of this thesis effort. I would also like to extend a special thank you to my committee chairperson for not giving up on me and assisting on occasion with the proverbial “size 10.” Additionally, I would be remised to not thank my Small Group Instructors, LTC Gordon Gore, Mr. Lowell Solien, Mr. Carey Walker, Mr. John Cary, and Mr. Maryln Pierce, for successfully implanting Mission Command into my vernacular this year. Most of all I would like to acknowledge the love and support of my wife and family; each of you has always been integral to my success.

TABLE OF CONTENTS

Page

ACRONYMS

CNCI	Comprehensive National Cybersecurity Initiative
DOD	Department of Defense
IA	Information Assurance
IT	Information Technology
NCCIC	National Cybersecurity and Communications Integration Center
NCIJTF	National Cyber Investigative Joint Task Force
TWI	Training with Industry
USCYBERCOM	United States Cyber Command

ILLUSTRATIONS

Page

TABLES

Page

CHAPTER 1

INTRODUCTION

> Government . . . operations depend on the network. If we lose that network we can't communicate, [and] . . . what happens when [adversaries] disrupt our network or the power grid or our banking institutions?[1]
>
> —General Keith B. Alexander, quoted in Pellerin, "Cybersecurity Involves Federal, Industry Partners, Allies"

The Problem

In recent years, the growth of the internet has established a means for Nation States, terrorist and criminal organizations, and individuals to launch attacks targeting the U.S. government and many major U.S.-based corporations. The intensifying threats and developing operational environment has led to an increased necessity to "trust" sister organizations across the United States government. Thus, the ever growing joint and inter-agency operations will begin to mold cyber soldiers and shift the dynamics of how the Armed Forces develop its future leaders of soldiers, sailors, airmen, and marines.

Primary Research Question

The complex operating environment of the cyber domain has created an increased necessity of joint missions and operations within cyberspace. Additionally, the last decade of combat has influenced the establishment of Mission Command. As a philosophy, Mission Command utilizes trust, mission orders, clear intent, and prudent risk to produce agile, adaptive leaders, who demonstrate disciplined initiative. Can Mission Command be applied to develop leaders of the Army's cyber warriors?

---

[1]GEN Keith B. Alexander, quoted in Cheryl Pellerin, "Cybersecurity Involves Federal, Industry Partners, Allies," *American Forces Press Service*, 8 November 2012, http://www.defense.gov/news/newsarticle.aspx?id=118479 (accessed 16 February 2013.

Secondary Research Questions

In order to further analyze the primary question, several other questions need to be addressed and answered. The questions below will also assist in identifying and analyzing the methods used to apply the philosophy of Mission Command to the development of the Army's cyber leaders.

1. In applying economy of force, are there areas of expertise and resources in the Joint and Inter-Agency environments the Army can and should rely on to develop its cyber warriors and leaders?
2. Can a joint and/or "whole of government" approach be applied in the development of future cyber leaders?
3. How can the current Army and Cyber/Communications culture benefit from embracing General Martin E. Dempsey's tenant of "trust" in the future operations?

Definitions

To gain a better appreciate for Mission Command within cyberspace as it relates to leader development, a few key words and terms need to be defined. The following words and terms are used throughout the course of the research paper. These key terms are used throughout the government, military, and commercial/private sector cyber communities when discussing the defense of information technology (IT) assets globally. These definitions are pulled from military doctrine.

Army Leader: "anyone who by virtue of assumed role or assigned responsibility inspires and influences people to accomplish organizational goals. Army leaders motivate

people both inside and outside the chain of command to pursue actions, focus thinking, and shape decisions for the greater good of the organization."[2]

Cyberspace: "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[3]

Cyberspace Operations: "the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid."[4]

Information Assurance: the "measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."[5]

Joint: "connotes activities, operations, organizations, etc., in which elements of two or more Military Departments participate."[6]

---

[2]Headquarters, Department of the Army, Army Doctrine Reference Publication (ADRP) 1-02, Change 2, *Operational Terms and Military Symbols* (Washington, DC: Government Printing Office, 28 November 2012), 1-3.

[3]Chairman of the Joint Chiefs of Staff, Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: Government Printing Office, 8 November 2010, as amended through 15 July 2011), 91-92.

[4]Ibid., 92.

[5]Ibid., 170-171.

[6]Ibid., 187.

Joint Operations: the general term to "describe military actions conducted by joint forces, or by Service forces in relationships (e.g., support, coordinating authority), which, of themselves, do not establish joint forces."[7]

Interagency: "United States Government agencies and departments, including the Department of Defense."[8]

Interoperability: the "ability to operate in synergy in the execution of assigned tasks. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases."[9]

Leader Development: a deliberate and progressive process, which cultivates soldiers into technically, and tactically proficient leaders capable of directing teams and organizations. Leader development transpires as a part of the lifelong combination of professional and civilian education, training, and overall experiences. Leader Development is dependent on three developmental domains: institutional, operational, and self-development, which are essential learning environments throughout a soldier's career.[10]

---

[7]Ibid., 196.

[8]Ibid., 179.

[9]Ibid., 182.

[10]Headquarters, Department of the Army, Army Doctrine Reference Publication (ADRP) 6-22, Change 1, *Army Leadership* (Washington, DC: Government Printing Office, 10 September 2012), 7-8 to 7-9.

> Army leaders must be self-aware and adaptive, comfortable with ambiguity, able to anticipate possible second- and third-order effects, and be multifunctional to exploit combined arms and joint integration. The Army uses resident, distributed, and blended education; training; and a mix of experiences and operational assignments.[11]

Lastly, Leader Development encompasses the mentoring, coaching, and counseling of all leaders within an organizational at all levels.

Operational Environment: "a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander."[12]

Philosophy of Mission Command: based on six principles; 1) build cohesive teams through mutual trust; 2) create shared understanding; 3) provide a clear commander's intent; 4) exercise disciplined initiative; 5) use mission orders; and 6) accept prudent risk.[13]

Limitations

The boundaries of this paper are restricted to leader development of cyber soldiers. The research addresses the philosophy of Mission Command as it relates to the structure and chain of command at the operational and strategic levels of command. Subsequently, the research will only relate key principles of leader development as

[11]Ibid., 7-9.

[12]Chairman of the Joint Chiefs of Staff, JP 1-02, 68.

[13]Headquarters, Department of the Army, Army Docrine Reference Publication (ADRP) 6-0, *Mission Command* (Washington, DC: Government Printing Office, 17 May 2012), 1-3.

described within Army doctrine. Lastly, the research is limited to the training and exercises at the operational and strategic level of operations.

Significance of this Research

As the Army becomes more dependent on technology, leader development is crucial to the future of the Army. Future Army leaders must embrace and execute the tenets of Mission Command throughout cyberspace. This research will demonstrate ways and means that Army leaders can and have implemented in order to facilitate the growth of young and future leaders. Additionally, this research is significant to government and military communities because of the expanding reliance on the digital environment and birth of Mission Command as a leadership philosophy.

Background

The following pages will describe the establishment of the United States Cyber Command (USCYBERCOM), as well as the development of Mission Command. It will center on each service's organizational structure and mission, why each organization was created, and how their mission is related to the defense of the cyber domain. It will also establish the operational environment for the study.

The New Beginnings

Technology and the digital environment have introduced and influenced one of the most dynamic and asymmetric battlefields of the 21st century. The World Wide Web presents an increased threat of what is referred to as "cyber based attacks." The ever expanding Department of Defense (DoD) digital resources, with over 15,000 computer networks across 4,000 military bases in 88 countries, has increased vulnerabilities which

have led to concerns over the segregation of these resources across the DoD and the Sister Services.[14]

In order to combine efforts, maximize joint capabilities, and capitalize on the military's cyber resources to combat the new emergent threat, the USCYBERCOM was established as a sub-unified command under the command and control of U.S. Strategic Command.

In a memorandum entitled, "Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations" (23 June 2009), the U.S. Secretary of Defense, Robert Gates, charged the newly formed command with the requirement to "synchroniz[e] warfighting effects across the global security environment as well as providing support to civil authorities and international partners."[15] USCYBERCOM was established as the driving force, charged with spearheading the integration of all DoD cyber resources operating in and around the cyber domain.

As military dependence on information systems and technology grows, so too does the liability, vulnerability, and threats to safeguarding the Nation's information infrastructure. In response to this emerging threat, the newly established USCYBERCOM has called for the creation of a new type of warrior–the "cyber soldier."

---

[14]Jordan Reimer, "U.S. Cyber Command Preparations Under Way, General Says," *American Forces Press Service*, 17 March 2010, http://www.af.mil/news/story.asp?id=123195306 (accessed 16 February 2013).

[15]Secretary of Defense, Memorandum, "Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations," 23 June 2009, http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyber_command_gates_memo[1].pdf (accessed 1 October 2012).

General Martin E. Dempsey, Chairman of the Joint Chiefs of Staff, emphasized that "Mission Command must be institutionalized and operationalized into all aspects of the joint force-our doctrine, our education, our training and our manpower and personnel processes."[16] As future operations begin to adapt to the "whole of government" concept of operations, this too will force design and structure reshaping of cyber warrior training and operations.

The ever growing joint and inter-agency operational environment, in conjunction with the increased necessity to trust sister organizations, will begin to mold the cyber warrior and shift the dynamics of how the Armed Forces train future soldiers, sailors, airmen, and marines. General Dempsey emphasized that "Mission Command for Joint Force 2020 requires trust at every echelon of the force."[17]

A Global Mission

Within the National Security Presidential Directive 54, *Cyber Security and Monitoring*, the U.S. Government defined cyber security as "prevention of damage to, protection of, and restoration of computers, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."[18]

---

[16]Martin Dempsey, *Mission Command White Paper*, Joint Chiefs of Staff, 3 April 2012, http://www.jcs.mil/content/files/2012-04/042312114128_CJCS_Mission_Command_White_Paper_2012_a.pdf (accessed 24 May 2013), 6.

[17]Ibid.

[18]Office of the Assistant Secretary of Defense for Networks and Information Integration/Departement of Defense Chief Information Officer, *Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance Strategy*, August

At the national level, the U.S. has established the National Cybersecurity and Communications Integration Center (NCCIC) and the National Cyber Investigative Joint Task Force (NCIJTF). While the NCIJTF is responsible for all domestic cyber threat investigations, the NCCIC mission is:

> to operate at the intersection of the private sector, civilian, law enforcement, intelligence, and defense communities, applying unique analytic perspectives, ensuring shared situational awareness, and orchestrating synchronized response efforts while protecting the Constitutional and privacy rights of Americans in both the cybersecurity and communications domains.[19]

USCYBERCOM is responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the DoD information networks. When required, they will conduct full-spectrum military cyberspace operations, in accordance with all applicable laws and regulations, in order to ensure U.S. and allied freedom of action in cyberspace, and protect these assets from our adversaries.[20]

Unlike its Sister Services, the U.S. Air Force has placed their dedication to the cyber fight up front within their overarching service mission statement: "Deliver sovereign options for the defense of the United States of America and its global interests – to fly and fight in Air, Space, and Cyberspace."[21] The 24th Air Force/U.S. Air Force

---

2009, http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf (accessed 14 May 2013), 1.

[19]U.S. Department of Homeland Security, "About the National Cybersecurity and Communications Integration Center," http://www.dhs.gov/about-national-cybersecurity-communications-integration-center (accessed 22 May 2013).

[20]U.S. Army Cyber Command/U.S. 2d Army, "United States Cyber Command Mission," http://www.arcyber.army.mil/org-uscc.html (accessed 14 October 2012).

[21]U.S. Air Force, "U.S. Air Force Mission Statement," http://www.af.mil/main/welcome.asp (accessed 24 October 2012).

Cyber Command's mission is to "extend, operate and defend the Air Force portion of the Department of Defense network and provide full spectrum capabilities for the Joint warfighter in, through and from cyberspace."[22]

In support of USCYBERCOM's global mission, the U.S. Army established and flagged U.S. Army Cyber Command (2d Army) in order to:

> plan, coordinate, integrate, synchronize, direct, and conduct network operations and defense of all Army networks; when directed, conduct cyberspace operations in support of full spectrum operations to ensure U.S./Allied freedom of action in cyberspace, and to deny the same to our adversaries.[23]

Thus, the U.S. Army Network Enterprise Technology Command/9th Signal Command (Army) remains the Army's execution arm and service provider to the Army, while simultaneously supporting Joint, Interagency, and Multinational network operations. NETCOM "plans, engineers, installs, integrates, protects, defends and operates Army Cyberspace, enabling Mission Command through all phases of Joint, Interagency, Intergovernmental and Multinational operations."[24]

The U.S. Navy Fleet Cyber Command mission is to:

> serve as central operational authority for networks, cryptologic/signals intelligence, information operations, cyber, electronic warfare, and space capabilities in support of forces afloat and ashore; . . . to direct, operate, maintain, secure, and defend the Navy's portion of the Global Information Grid; . . . to assess Navy cyber readiness; to manage man, train, and equip functions associated with Navy Component Commander and Service Cryptologic

---

[22]24th Air Force, "24th Air Force Fact Sheet," 3 January 2013, http://www.24af.af.mil/library/factsheets/factsheet.asp?id=15663 (accessed 3 April 2013).

[23]U.S. Army Cyber Command/U.S. 2d Army.

[24]U.S. Army Network Enterprise Technology Command, "NETCOM Mission and Vision," http://www.army.mil/info/organization/unitsandcommands/command structure/netcom/ (accessed 14 October 2012).

> Commander responsibilities; and to exercise administrative and operational control of assigned forces.[25]

In conjunction, the U.S. 10th Fleet serves as the Navy's numbered fleet for Fleet Cyber Command, as well as executes "operational control of assigned Naval forces; to coordinate with other naval, coalition and Joint Task Forces to execute the full spectrum of cyber, electronic warfare, information operations and signal intelligence capabilities and missions across the cyber, electromagnetic and space domains."[26]

The Global Threat

> Both state and non-state actors possess the capability and intent to conduct cyber espionage and, potentially, cyber attacks on the United States, with possible severe effects on both our military operations and our homeland.[27]

In recent years, Nation States, terrorist and criminal organizations, and individuals have utilized the internet and cyber domain to launch attacks–kinetic and information–against the U.S. government, as well as many major U.S.-based corporations. Adversaries of the U.S. understand the exponential and expansive power possessed within the World Wide Web. Furthermore, state-sponsored hackers, particularly from China and Iran, have targeted noteworthy computer networks within the U.S.[28] Additionally, evidence has

---

[25]U.S. Fleet Cyber Command, U.S. 10th Fleet, "U.S. Fleet Cyber Command Mission and U.S. Tenth Fleet Mission," http://www.fcc.navy.mil/ (accessed 14 October 2012).

[26]Ibid.

[27]Departement of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, January 2013, http://iase.disa.mil/policy-guidance/dasd_ciia__ strategy_aug2009.pdf (accessed 12 May 2013), 3.

[28]Michael Leiter, "Analysis: As Cyberthreat Looms, Here's What Really Matters," NBCNews.com, 22 February 2013, http://usnews.nbcnews.com/_news/2013/

shown several countries, such as China and Russia, have developed their own cyber forces. Of critical significance, China established cyber formations, with key goals, objectives, and missions, in order to identify and exploit weaknesses within the U.S. military, government, and commercial cyber infrastructure.[29]

The asymmetric and uninhibited dynamics of cyberspace have opened up an infinite sum of uses for terrorist and organized crime syndicates. In turn, the cyber domain has enabled non-nation state elements a greater span and audience in order to recruit new members and inspire their supporters. Subsequently, "they [terrorists] can operate essentially unrestrained and are free to innovate, unbound by law, policy, or precedent."[30]

A Global Common

> The United States requires freedom of action in the global commons and strategic access to important regions of the world to meet our national security needs.[31]

Global commons are "the earth's unowned natural resources, such as the oceans, the atmosphere, and space."[32] In contrast, the U.S. DoD included cyberspace to the list of global commons and a key national interest, as early as 2005.[33]

02/22/17057322-analysis-as-cyberthreat-looms-heres-what-really-matters?lite (accessed 24 February 2013).

[29]Keith B. Alexander, "Warfighting in Cyberspace," *Joint Forces Quarterly* no. 46 (3d Quarter 2007): 59, http://www.carlisle.army.mil/DIME/documents/Alexander.pdf (accessed 5 June 2013).

[30]Ibid.

[31]Department of Defense, *National Defense Strategy* (Washington, DC: Government Printing Office, June 2008), http://www.defense.gov/news/2008%20National%20Defense%20Strategy.pdf (accessed 4 June 2013), 16.

The concept of the global commons was conceived in order to identify resource domains in which all sovereign nations, organizations, and individuals have legal access and freedom of use. The internationally accepted global commons of air, sea, and space have been defined through international laws and treaties.

In December 1970, The United Nations Convention on the Law of the Sea established globally accepted laws of the high seas, while defining sovereign coastal waters and the Exclusive Economic Zone for nations. Subsequently in the years to follow, the United Nations Convention met on numerous occasions until the Convention was entered into decree per Article 308 on 16 November 1994. To this day, the Convention is still renowned and globally recognized as the premier organization to mediate all matters relating to the law of the sea.

In the mid-1940s, the International Civil Aviation Organization, a specialized agency of the United Nations, and the International Air Transport Association were the first global organizations established in order to set and enforce standards and regulations necessary for safe use of the skies.[34] Additionally, these organizations created the means for the international community to collaborate in order to improve air travel for the good of individuals around the world.

---

[32]Oxford Dictionaries, "Global Commons," http://oxforddictionaries.com/us/definition/american_english/global%2Bcommons (accessed 17 March 2013).

[33]Department of Defense, *The Strategy for Homeland Defense and Civil Support* (Washington, DC: Government Printing Office, June 2005), http://www.defense.gov/news/Jun2005/d20050630homeland.pdf (accessed 17 March 2013), 12.

[34]International Air Transport Association, "The Early Days," http://www.iata.org/about/Pages/history_2.aspx (accessed 1 May 2013).

With the launch of the world's first satellite into outer space, Russia's Sputnik set into motion the world's desire to recognize the space domain as a global common. Subsequently, the United Nations and the Outer Space Treaty of 1967 defined outer space and set the foundation for the establishment of international laws governing space activities.[35]

The international acceptance and development of cyberspace as a global common will first define the legality–Law of Armed Conflict, *jus ad bellum*, and *jus in bello*–in the application of offensive and defensive cyber warfare. It will also establish a conduit for international collaboration in order to share best practices and safe deployment for the defense of cyber activity worldwide.

The shared international practices of global commons–air, sea, and space–throughout the last 60 years have established the necessary means for shared knowledge, trust, and security for national assets, commercial businesses and organizations, and individuals globally. These same principles are in keeping with the key attributes of the philosophy of Mission Command–shared standards and common understanding through doctrine, education, training, and processes.

Summary

In an era of digital enhancements and interdependence, the development of cyberspace has brought forth a new threat to the national interests and assets of the U.S. Subsequently, the U.S., DoD, and the Army have established new technology,

[35]United Nations, *United Nations Treaties and Principles On Outer Space, related General Assembly, resolutions and other documents*, http://www.unoosa.org/pdf/publications/st_space_61E.pdf (accessed 1 May 2013).

formations, and doctrine in order to effectively maximize their ability to operate and defend operations within the cyber domain. While exploiting lessons learned over the past 12 years, the philosophy of Mission Command and leader development have proven critical to the advancement of future success in cyberspace operations.

CHAPTER 2

LITERATURE REVIEW

There are numerous resources of information on cyber training and Mission Command within the military, including articles, manuals, and Congressional articles, though none directly address the application of Mission Command to the development of cyber soldiers and leaders. These documents address the role and importance of the nation's security as it relates to the ability to effectively defend and operate in cyberspace.

This chapter will outline some of the key documents, while chapter 4 will provide a more in depth examination of the importance and application in order to provide a prospective solution to the research questions. The literature is separated into two major categories. The first category involves government documents, articles, and research studies focused on the establishment of USCYBERCOM and cyber training. The second category consists of doctrine and professional papers focused on Mission Command and leader development.

Category 1–Cyber Training

USCYBERCOM is responsible for the overall organizing, training, and equipping of the DoD cyber forces, and has passed the same responsibilities to the service commands for their respective cyber command formations. In September 2010, Lieutenant General Rhett A. Hernandez, U.S. Army Forces Cyber Command Commander, addressed the importance of cyber training and how “we must therefore make significant investments in education, training, and experience to understand

emerging trends, develop and deploy new capabilities, and effectively defend against new cyberspace threats."[36]

Lieutenant General Hernandez went on to emphasize the importance and roles ARFORCYBER will play in support of USCYBERCOM, the Component Commands, Sister Service Components, other government departments and agencies, as well as within the private sector. For ARFORCYBER to achieve success, the Army must establish processes and procedures to consistently and habitually share operational data, situational awareness, planning, and resources with all Services, departments, and agencies operating in cyberspace.

As part of the "Comprehensive National Cybersecurity Initiative (CNCI)," President Barack Obama identified cyber security as one of the top security challenges facing the Nation today and in the near future. The President reiterated concerns that the Nation as a whole is currently not poised to dominate the cyber domain, and must take significant steps across the government and civilian community to combat cyber threats today and in the future. The CNCI consists of 12 mutually supporting and reinforcing initiatives aimed at achieving three primary goals: (1) establish a defense against immediate threats; (2) defend against the full spectrum of threats; and (3) strengthen the future cyber security environment. Most notable of these initiatives are: "Initiative #1,

[36]U.S. Congress, House, "Statement of Major General Rhett Hernandez, USA, Incoming Commanding General, U.S. Army Forces Cyber Command before the House Armed Services Committee, Subcommittee on Terrorism, Unconventional Threats and Capabilities," 111th Cong., 2nd sess., 23 September 2010, http://democrats.armed services.house.gov/index.cfm/files/serve?File_id=067ffc96-e5c1-4cef-baa2-010d16e3be57 (accessed 24 September 2012).

manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections, and Initiative #8, expand cyber education."[37]

The National Cyber Incident Response Plan provides the national framework for cyber incident response. The National Cyber Incident Response Plan outlines the roles and responsibilities for all government agencies in defending national interests in the cyber domain. Furthermore, the plan correlates national policy and doctrine into a single concept for planning and executing cyber operations in the defense of cyberspace, as well as recovery and response procedures to cyber attacks. This document is the U.S. strategic plan for operational coordination and execution between the government, private sector, and international partners. Lastly, the plan establishes how the government will centralize coordination, while decentralizing computer network operations/computer network defense.[38]

DoD Directive 8570.01-M, *Information Assurance Workforce Improvement Program,* is the guiding manual for the management of Information Assurance (IA) personnel throughout the DoD in accordance with DoD Directive 8570.01, *Information Assurance Training, Certification, and Workforce Management.* DoD 8570.01 establishes

[37]The White House, "The Comprehensive National Cybersecurity Initiative," National Security Council, 19 February 2013, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (accessed 20 October 2012).

[38]Department of Homeland Security, *National Cyber Incident Response Plan*, Interim Version, September 2010, http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf (accessed 18 May 2013).

the common baseline training requirements for all IA personnel throughout the DoD, as well as defining the roles and responsibilities of IA personnel.[39]

The *Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance Strategy* outlines the DoD's overarching strategy for the defense for Cyber, Identity and Information Assurance. The DoD objective targets influencing subordinate components and supporting all business, warfighting, and intelligence missions, which includes all Joint Capability Areas. Additionally, the Cyber, Identity and Information Assurance explicitly focuses on computer network operations, with emphasis on network defense and IA tasks. Furthermore, figure 1 shows Cyber, Identify and Information Assurance's vision to promote "freedom of action in cyberspace" through four key goals, which allow for near-term success, long-term investment, and an overall synergistic and unified vision across the entirety of the DoD.[40]

[39]Department of Defense, Department of Defense 8570.01-M, *Information Assurance Workforce Improvement Program,* 24 January 2012, http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf (accessed 14 May 2013).

[40]Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer, *Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance Strategy*, V.

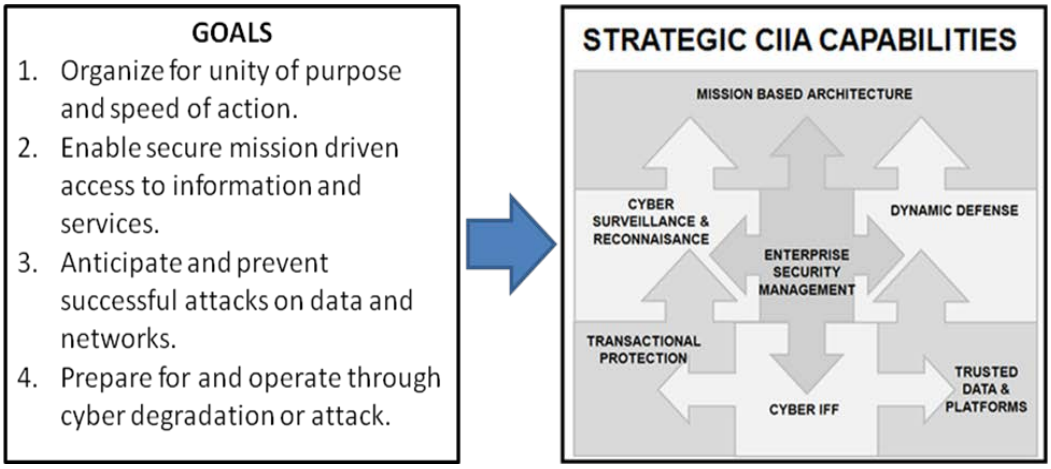


Figure 1. CIIA Vision and Strategy

Source: Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer, *Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance Strategy*, August 2009, http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf (accessed 14 May 2013), V.

In *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, the DoD outlines its most recent strategic guidance for the military forces. Within its strategy, the DoD supports the national strategy in both areas of the cyber domain and Mission Command. Along with summarizing the importance of operating effectively in cyberspace, the defense strategy stresses the importance of continued efforts to exploit domestic and international allies' competencies in order to further advance the DoD's overall capabilities to defend the networks. In addition, the DoD strategy expounds on its requirement to preserve and capitalize on the key advancements in the military's interdependence to operate as a joint force.[41] "The United States faces profound challenges that require strong, agile, and capable military forces whose actions are

[41]Departement of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, 8.

harmonized with other elements of U.S. national power . . . The balance between available resources and our security needs has never been more delicate."[42]

In the U.S. Army *2013 Posture Statement* to the Senate Armed Services Committee, Secretary of the Army John M. McHugh and General Raymond T. Odierno outlined the current state and future direction of the Army. Within their statement, they explained the Army's capability to align efforts per the national strategy of the President and DoD. Additionally, they accentuated the importance of the LandWarNet, and its criticality to providing the right information at the right time, thus allowing leaders and soldiers the ability to make the essential decisions on the battlefield. Subsequently, they emphasized the significance of the Army's efforts in establishing a "single, secure, standards-based, versatile network that connects Soldiers and their equipment to vital information and our Joint, interagency, intergovernmental and multinational partners."[43] Furthermore, the *Army Posture Statement* explains the Army's contributions to the Joint force in line with Mission Command. Most notably are the Army's cyberspace contributions: "We [United States Army] build and operate the space and terrestrial communication networks that connect our own units, the Joint community, and interagency and multinational partners." [44]

---

[42]Ibid.

[43]U.S. Congress, Senate Armed Services Committee, "Statement of Secretary of the Army John M. McHugh and General Raymond T. Odierno," 113th Cong., 1st sess., 23 April 2013, 17.

[44]U.S. Congress, Senate Armed Services Committee, "Statement of Secretary of the Army John M. McHugh and General Raymond T. Odierno," 7.

Major Andrew Hansen's thesis research outlines the importance and benefits of conducting cyberspace training exercises at the tactical, operational, and strategic levels. Additionally, he focuses on the need for a dedicated realistic, joint, flag level exercise in order to capitalize on previously established cyber exercises lessons learned, while concurrently establishing the importance of the U.S. military's requirement for dominance throughout the cyber domain.[45]

In his article, "The Next Battlefield: The Reality of Virtual Threats," Michael Vitas describes the importance of shared global understanding of the operating environment of cyberspace for the U.S. government as a whole. He further described the necessity for shared awareness of ways and means in which the cyber domain is used to conduct cyber terrorism, cyber espionage, cyber warfare, and cyber attacks. Given the intense speed and severity with which these operations can be carried out, the U.S. must be prepared to respond swiftly, efficiently, and effectively. U.S. government departments and agencies share the burden to protect the vital interests of the government and its people.[46]

From approximately 1999 to 2002, III Corps signal units spearheaded the fielding, training, and implementation of the Army's first digital Corps. In "Bridging the 'digital delta': Training III Corps Signaleers," Colonel Dennis Via and Major Linda Jantzen characterize one of the essential keys to transforming communications training

[45]Maj Andrew P. Hansen, USAF, "Cyber Flag: A Realistic Cyberspace Training Construct," Air Force Institute of Technology, Wright Patterson Air Force Base, OH, March 2008, 60-62.

[46]Michael Vitas, "The Next Battlefield: The Reality of Virtual Threats," *Global Catastrophe* 28, no. 3 (Fall 2006): 3-6, http://www.nyu.edu/intercep/lapietra/Vatis_TheNextBattlefieldTheRealityofVirtualThreats.pdf (accessed 20 October 2012).

throughout the Corps was centralized control by the III Corps G6 , while decentralizing execution. They go on to emphasize the shared responsibility of signal commands, government agencies, and industry in the sustained training of signaleers. Signal units must provide training for newly arrived soldiers in order to establish the requesant baseline knowledge and training, while establishing refresher courses to sustain the required level of proficiency desired. Signal units will use the Soldier Development Center to facilitate their leader development and individual training programs. It provides soldiers the ability to participate in degree programs, computer-based training, and distance-learning programs for signal military occupational specialty. Digital-training requirements in III Corps demand resources far greater than any unit with an operational mission can support.[47]

In "Cybersecurity Involves Federal, Industry Partners, Allies," Cheryl Pelleri explains many of the key concerns that Army General Keith Alexander, Commander of CYBERCOM and Director of the National Security Agency, discussed as part of a speaking engagement during the Symantec 2012 Government Symposium. The article emphasizes the interdependence of the DoD, Department of Homeland Security, National Security Agency, Federal Bureau of Investigation, and other government agencies, along with leading commercial cyber/network defense companies, on the overall defense of the nation and world's cyber domain. Additionally, General Alexander went on to stress that "Government . . . operations depend on the network. If we lose that network we can't

[47]COL Dennis Via and MAJ Linda Jantzen, "Bridging the 'Digital Delta': Training III Corps Signaleers," *Army Communicator* 27, no. 2 (Summer 2002): 44.

communicate, [and] . . . what happens when [adversaries] disrupt our network or the power grid or our banking institutions?"[48]

In their article, "Exploiting the Potential of Cyber Operations," Felix Juhl and Heiko Borchert break down potential operational, strategic, psychological and special effects that can be achieved through cyber operations in future engagements. Furthermore, they explain the importance of synchronization, coordination, and training required by forces in order to capitalize on effects attained throughout cyber operations, and how they correspond to the battlefield, and how they are to be exploited on the battlefield.[49]

As an article in a part series, "Cyberspace as Global Commons," Dr. Kamlesh Bajaj, CEO of Data Security Council of India, argues that the cyber domain needs to be treated as both a national asset and a global domain. Dr. Bajaj also outlines the challenges nations and the world have in operating within cyberspace, as well as protecting its national assets spread across the global information grid. Furthermore, he points out the necessity of the international community to define the legality – Law of Armed Conflict, *jus ad bellum,* and *jus in bello* – in the application of offensive and defensive cyber warfare. Additionally, Dr. Bajaj discusses the need for a shared international environment

[48]Cheryl Pellerin, "Cybersecurity Involves Federal, Industry Partners, Allies," *American Forces Press Service*, 8 November 2012, http://www.defense.gov/news/newsarticle.aspx?id=118479 (accessed 16 February 2013).

[49]Felix Juhl and Heiko Borchert, "Exploiting the Potential of Cyber Operations," *Jane's Defence Weekly* 48, no. 26 (29 June 2011): 22, https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=News&ItemId=+++1187350&Pubabbrev=JDW (accessed 19 February 2013).

in order to discuss, collaborate, and protect against cyber threats and associated vulnerabilities and attack vectors.[50]

Category 2–Mission Command and Leader Development

The U.S. Army Center of Excellence for Mission Command has published a multitude of documents and manuals on Mission Command as both a philosophy and a warfighting function. Army Doctrine Reference Publication (ADRP) 6-0, *Mission Command*, and Field Manual (FM) 6-0, *Mission Command*, provide the foundation of mission command, though recent articles, like those of Colonel Thomas Guthrie and Lieutenant General Robert Caslen, place into context the intent of Mission Command.

In Lieutenant General Robert Caslen and Colonel Charles Flynn's article, "Introducing the Mission Command Center of Excellence," they state, "making mission command institutional requires appropriate changes in doctrine and training." In turn, one of the key tenets of the Mission Command Center of Excellence is to fully integrate mission command into the Army's doctrine, organization, training, material, leader development and education, personnel, and facilities.[51]

As stated in ADRP 6-0, "mission command is based on mutual trust and a shared understanding and purpose between commanders, subordinates, staffs, and unified action

[50]Kamlesh Bajaj, "Cyberspace as Global Commons," *Dataquest*, General OneFile, 14 May 2012, http://go.galegroup.com.lumen.cgsccarl.com/ps/i.do?id=GALE%7CA289665832&v=2.1&u=97mwrlib&it=r&p=ITOF&sw=w (accessed 5 June 2013).

[51]LTG Robert L. Caslen, Jr. and COL(P) Charles A. Flynn, "Introducing the Mission Command Center of Excellence," *Army* 61, no. 2 (February 2011): 53-56, http://www.ausa.org/publications/armymagazine/archive/2011/2/Documents/Caslen_Flynn_0211.pdf (accessed 24 September 2012).

partners. It requires every soldier to be prepared to assume responsibility, maintain unity of effort, take prudent action, and act resourcefully within the commander's intent."

The "mutual trust and shared understanding" across the spectrum of departments, agencies, and Services operating in cyberspace starts at the training, education, and doctrine level. Additionally, U.S. Army doctrine on Mission Command explicitly discusses the balance of the art of command with the science of control, and how a commander must exercise each when leading and training their soldiers.[52]

ADP 6-0, *Mission Command* more specifically defines the six key principles of Mission Command: (1) build cohesive teams through mutual trust; (2) create shared understanding; (3) provide a clear commander's intent; (4) exercise disciplined initiative; (5) use mission orders; and (6) accept prudent risk. Furthermore, ADP 6-0 describes a commander's responsibility to establish a unit culture that guides and facilitates the development of subordinate leaders. Additionally, a commander will shape proficient teams through mutual trust and provide a shared understanding throughout the organization by providing clear intent and mission orders.[53]

U.S. Air Force doctrine, Air Force Doctrine Document (AFDD) 6, *Command and Control*, provides guidance to the Air Force's "total force" on executing command and control operations, while emphasizing the need for diverse, interoperable command and control centers and appropriately trained Airmen capable of supporting a full spectrum of requirements worldwide. "We organize, train, and equip Airmen to execute the myriad

[52]Headquarters, Department of the Army, ADRP 6-0, 2-1.

[53]Ibid., 2-1 to 2-5.

tasks of command and control of air, space, and cyberspace forces through Air Force global and theater command and control systems."[54]

The U.S. Marine Corps doctrine, Marine Corps Doctrinal Publication (MCDP) 6, *Command and Control*, describes effective commands as those who execute and promote unrestricted communications, thus executing the free flow and sharing of significant information throughout the organization. The Marine Corps command and control system supports the ability to create tempo, flexibility, and the ability to exploit opportunities, while subsequently decentralizing orders and relying on disciplined initiative. "Whatever the age or technology, effective command and control will come down to people using information to decide and act wisely. And whatever the age or technology, the ultimate measure of command and control effectiveness will always be the same: Can it help us act faster and more effectively than the enemy?"[55] Lastly, the Marine Corps command and control doctrine emphasizes the role of training and education in the preparation for future operations.

Department of the Army Pamphlet (DA Pam) 350–58, *Army Leader Development Program* (ALDP), outlines the Army's processes for leader development at all levels. It serves as a guide for commanders and leaders responsible to the development of officers, warrant officers, and noncommissioned officers of the Active Army Component, the Army National Guard, and the Army Reserve. It defines the Army's methodology and

[54]U.S. Air Force, Air Force Doctrine Document (AFDD) 2-8, *Command and Control* (Washington, DC: Air Force Departmental Publishing Office, 1 June 2007), foreword.

[55]U.S. Marine Corps, Marine Corps Doctrinal Publication (MCDP) 6, *Command and Control* (Quantico, VA: Secretary of the Navy, 4 October 1996), 60.

processes used to manage the three pillars of leader development. Figure 2, below, illustrates the role the three foundations of leader development play within each of the domains.[56]

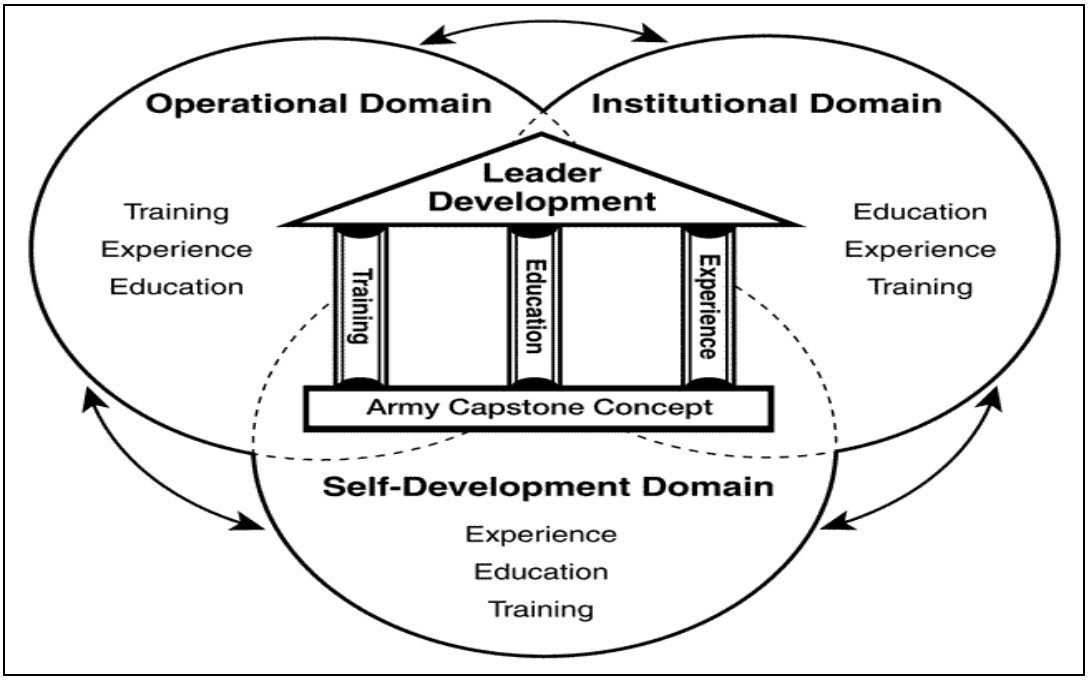


Figure 2. Army's Leader Development Model

Source: Headquarters, Department of the Army, Department of the Army Pamphlet (DA PAM) 350-8, *Army Leader Development Program* (Washington, DC: Government Printing Office, 8 March 2013), 2.

ADRP 6-22, *Army Leadership*, establishes and outlines the roles and responsibilities of leaders within the U.S. Army, while supporting the principles of

[56]Headquarters, Department of the Army, Department of the Army Pamphlet (DA PAM) 350-8, *Army Leader Development Program* (Washington, DC: Government Printing Office, 8 March 2013), 1.

Mission Command. Along with describing key leader attributes, the manual institutes the foundation for all leaders: officer, warrant officer, non-commissioned officer, and civilian alike. Additionally, it sets the stage and expectations for the core competencies of a leader across all levels. Lastly, it forms the basis and describes basic principles for leader development through counseling, coaching, and mentoring.[57]

Summary

While research of cyberspace and Mission Command are still fairly immature, there was ample information on cyber training and Mission Command within military journals, doctrine, Congressional statements and audits, and professional articles. No direct research data currently addresses the application of Mission Command to the development of cyber soldiers and leaders. There was adequate data on the national and strategic vision for the future of cyberspace to include: (1) the current posture of the U.S. and cyberspace; (2) the organizations within the U.S. established to defend and defeat the cyber threat; and (3) education opportunities for cyber warriors. The next chapter will outline the research methodology used in order to analyze the data collected, and answer the research questions.

[57]Headquarters, Department of the Army, ADRP 6-22, v.

CHAPTER 3

RESEARCH METHODOLOGY

The research methodology consists of analyzing the application of Mission Command doctrine to the leader training and development of the nation's cyber soldiers. The data collection tested the application of Mission Command, focused on the concepts as a philosophy, in the analysis of developing officers and non-commissioned officers throughout the communications and cyber communities within the Army. Additionally, the researcher collected empirical and qualitative data for analysis.

In addition, the research analyzed the philosophy of Mission Command as it applied to U.S. organizational structure, inter-agency exercises, and other training related to cyber defense and operations. The research further analyzed the DoD and Department of the Army structures, cyber exercises, and other training related to cyber defense and operations as it applies to the philosophy of Mission Command.

The analysis of the joint and inter-agency environment provided an output and understanding of the tools and capabilities the Army has capitalized on from government agencies and Sister Services in order to further develop their cyber leaders. Furthermore, it provided an understanding of government agencies operating under the "whole of government" concept in the application of cyber operations.

Secondly, an analytical review of ways in which the current Army and Cyber/Communications culture are embracing General Dempsey's key tenant of trust within the current structure, exercises, and training related to cyber defense and operations. Additionally, it provided assets for the sustainment or improvement of leader development through trust with the Sister Services and governmental agencies during

future operations. Lastly, the research analyzed the areas of expertise and resources resident within the Joint, Inter-Agency, and commercial environments in which the Army can capitalize on in order to further the development of their cyber leaders.

Research Planned But Not Executed

The researcher planned to analyze the individual training plans/syllabi for cyber soldiers for each of the service's cyber schools. The researcher concluded that the information would focus more at the individual and tactical level. Thus, the information would be outside the scope of the research.

Summary

The research methodology consisted of analyzing the application of Mission Command doctrine to the leader training and development of the nation's cyber soldiers. The empirical and qualitative data collected tested the application of Mission Command as it applies to leader development.

CHAPTER 4

ANALYSIS

> Confronted with a task, and having less information available than is needed to perform that task, an organization may react in either of two ways, One is to increase its information processing capacity, the other to design the organization, and indeed the task itself in such a way as to enable it to operate on the basis of less information. . . . a failure to adopt one or the other will automatically result in a drop in the level of performance.[58]
>
> — Martin van Creveld, *Command in War*

This chapter is divides into two major sections. The first section of the chapter addresses the analysis of empirical and qualitative data essential to answer the primary research question. The second section of this chapter revisits the research data in order to address the secondary questions, and support the proposed recommendations in chapter 5.

Primary Research Analysis

> Organization, as much as a battleship or a bayonet, is a weapon of war.[59]

The philosophy of Mission Command guides commanders through the development of their organization's leader development plans. While harmonizing the art and science of command, commanders balance the three pillars of leader development, training, education, and experience, with a prudent level of risk to the organization, as well as the individual leader. The training and development of cyber warriors and leaders are no exception. This section will address how strategic and operational level

[58]Martin van Creveld, *Command in War*, quoted in U.S. Marine Corps, MCDP 6, 61.

[59]COL (ret) Martin van Creveld, quoted in LTC Frank J. Snyder, "Incorporating Cyber in Exercises" (Slide Presentation, U.S. Pacific Command, 15 August 2012).

organizational structure, education, and training can facilitate the interdependence of Mission Command and leader development.

Organizational Structure

Organizational structure supports four of Mission Command's key tenets. First, it supports a commander's ability to establish a culture and command climate, which invites the building of cohesive teams through mutual trust within the organization. Secondly, command relationships support and facilitate the organization's common operating picture and create a shared understanding of the operating environment. Lastly, command structure and relationships facilitate a commander's ability to issue a clear intent through mission orders.

In combination, the culture and command climate of an organization is vital to the development of its leaders. A tactically and technically proficient organization will produce proficient leaders within their career field and the Army. In an operating environment such as cyberspace, technically proficient leaders are the cornerstone for mission accomplishment, as well as vital to the progression of the organization. Trust between organizational leaders is a critical foundation to the growth of its leaders. In an operating environment unconstrained by borders, trust becomes an essential tenet to the organizational structure and overall defense of the nation's network and crucial assets.

The DoD computing environment consists of 4,000 installations, 21 satellite gateways, 7 million computers, 120,000 commercial circuits, and 15,000 networks. As a result, the DoD must defends its assets from approximately 360 million probes a day

from hackers, nation states, insiders, terrorists, and criminals alike. In comparison, a single major bank within the U.S. will encounter nearly one million probes per month.[60]

As cyber threats increased and the reliance of national assets on the cyber domain grew, the U.S. government acknowledged the need to establish organizations dedicated to the defense of the nation's overall security within cyberspace. In June 2009, the DoD established USCYBERCOM in order to support the nation's strategic security policy. The DoD and USCYBERCOM are only components within the nation's overall defense of the cyber domain.

[60]Don Davidson, *Comprehensive National Cyber Security Initiative (CNCI) & ICT Supply Chain Risk Management (SCRM)*, National Defense Industrial Association Logistics, 16 October 2009, http://www.ndia.org/Divisions/Divisions/Logistics/Documents/DD%20at%20NDIA%20Log%2016oct.pdf (accessed 10 May 2013).

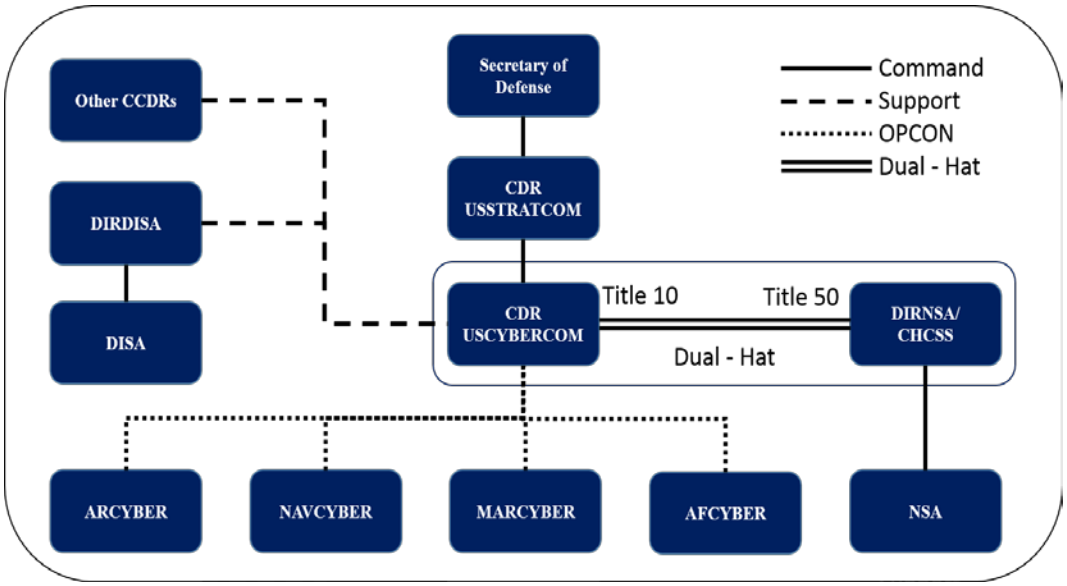


Figure 3. U.S. Cyber Command Organization

Source: Created by author; derived from Vincent Van Houten, "An Overview of the Cyber Warfare, Exploitation & Information Dominance (CWEID) Lab," Systems Center Atlantic, 28 January 2010, http://info.publicintelligence.net/cyberwarfarebrief.pdf (accessed 17 May 2013).

The combined efforts, maximizing of defense capabilities, and exploitation of cyber resources within the DoD are evident at the strategic and national level. Figure 4 depicts the strategic level coordination and command relationships within the DoD. The critical command relations with USCYBERCOM are: (1) the Commander, USCYBERCOM is also dual-hatted as the Director of the National Security Agency; (2) the service component cyber units are operationally controlled by USCYBERCOM; and (3) there is a support relationship between USCYBERCOM and both Defense Information Systems Agency and the nine other Combatant Commands. Though prior to fully analyzing the national command and control structure for defending the cyber

domain, the U.S. Codes governing legalities and authorities must be addressed. There are three major U.S. Codes that govern key agencies responsible for cyber operations.

First, Title 10 applies directly to military operations. Additionally, it establishes the Secretary of Defense with the authority to direct and control the DoD, to include all organizations subordinated to the Office of the Secretary of Defense. Second, Title 50 outlines government authority to conduct foreign intelligence reconnaissance, surveillance, and collection. Title 50 is most notably associated with intelligence agencies, such as National Security Agency, Defense Intelligence Agency, and the Central Intelligence Agency. Lastly, the Department of Homeland Security and Department of Justice execute Title 18 responsibilities, and are responsible for the security of government networks, as well as executing the national authority for federal law enforcement activities under Title 18.

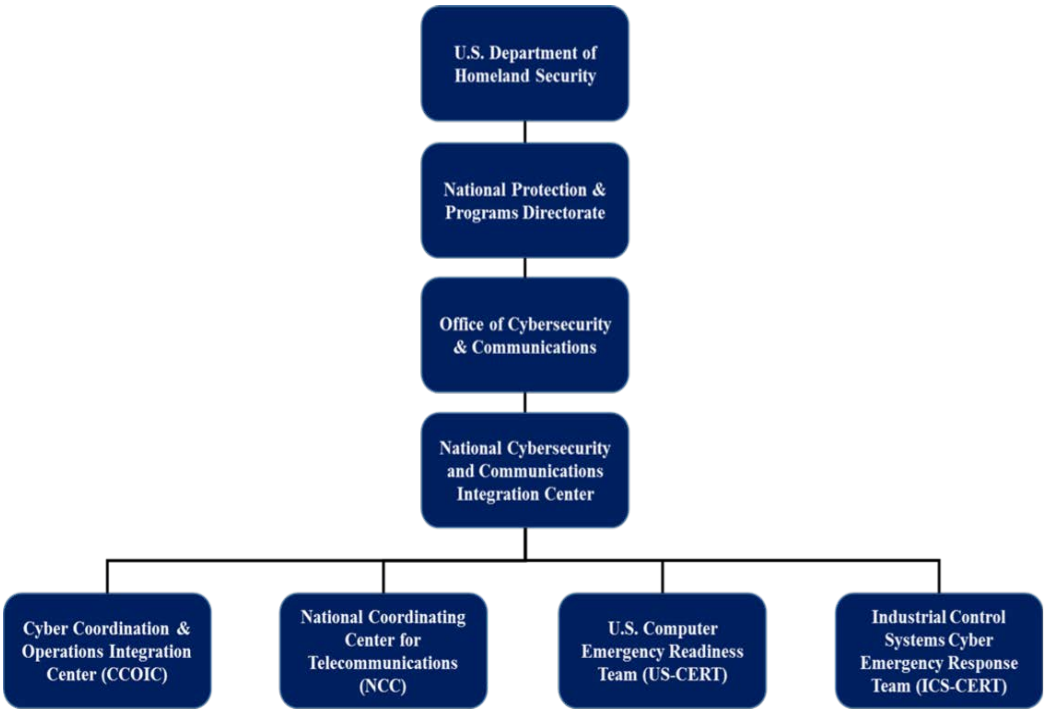
While each title applies to the execution of defending U.S. national interests and assets in cyberspace, they limit the authority to operate outside of their specified area of responsibility. The Congressional limitations make it difficult for government agencies to optimize an economy of force and resource, without fear of violating congressional mandates for separation of activities. However, national entities, such as the NCIJTF and NCCIC, have been established to provide a singular common operating picture and shared understanding of vulnerabilities, intrusions, incidents, mitigation, and recovery actions for national communications and cybersecurity assets.

While relying heavily on collaboration with its partners, the NCCIC coordinates with all federal agencies and departments in order to secure the government's cyber operating environment. Additionally, it solicits the private sector and international

counterparts. For example, the Conficker worm was discovered at Stanford University in 2008. The discovery impelled top computer/internet security experts to establish a working group in order to better identify the origin and subsequent target of the malicious code. Private working groups and corporations continue to work with "the government to secure vital computer networks from botnets like Conficker."[61] Despite operating a national coordination cell, the protection of the nation's critical assets and cyber domain relies on the mutual trust each organization, department, and agency have in one another to do their due diligence to safeguard cyberspace.[62] Figure 4 illustrates the vastness of the NCCIC, while supporting its ability to pull expert resources together, collaborate, and share a common understanding of the state of cyberspace.

[61]Mark Bowden, "The 'Worm' That Could Bring Down The Internet," NPR Books, 27 September 2011, http://www.npr.org/2011/09/27/140704494/the-worm-that-could-bring-down-the-internet (accessed 29 May 2013).

[62]Official Website of Homeland Security.



NCCIC Partners

Other elements of DHS - United States Coast Guard - FEMA, NRCC, and FEMA Operations Center	National Telecommunications and Information Administration (NTIA)	Electricity Sector Information Sharing and Analysis Center
Department of Defense	Department of Energy	Financial Services Information Sharing and Analysis Center
National Security Agency	Department of Transportation/Federal Aviation Administration Cyber Security Management Center	Council of Information Sharing and Analysis Centers
Other elements of the Intelligence Community	National Communications System (all 24 departments and agencies)	Information Technology Information Sharing and Analysis Center
Department of Justice	Elements of other departments and agencies	Multi-State Information Sharing and Analysis Center
Department of State	Executive Office of the President	Water Information Sharing and Analysis Center
Department of Treasury	Additional ISACs and other sector-designated organizations upon request	Communications Infrastructure Information Sharing and Analysis Center
Department of Commerce	Individual owners and operators of cybersecurity and communications CIKR, upon request and by agreement	National Response Coordination Center
National Institute for Standards and Technology (NIST)	Owners and operators of Legislative Branch and Judicial Branch networks upon request.	Immigration and Customs Enforcement Cyber Crime Center
National Operations Center	National Cyber Investigative Joint Task Force	NSA/CSS Threat Operations Center
National Infrastructure Coordinating Center	Intelligence Community - Incident Response Center	United States Secret Service
	National Cyber Security Center	

Figure 4. National Cybersecurity and Communications Integration Center Organization and Partners

Source: Created by author.

With General Keith Alexander dual-hatted as the Commander of USCYBERCOM and Director of the National Security Agency, the DoD command

structure for cyber operations supports a unified command strategy, promotes a clear commander's intent, and enables nesting of the DoD cyber mission with the National Command Authority's strategy.

In January 2008, President Barack Obama updated the national U.S. cyber security strategy and endorsed the most recent version of the National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23). As part of the CNCI, NSPD-54/HSPD-23 established the NCIJTF, and directed the NCIJTF to coordinate, integrate, and share information related to all domestic cyber threat investigations.[63]

[63]U.S. Department of Justice, "National Cyber Investigative Joint Task Force," Federal Bureau of Investigation, http://www.fbi.gov/about-us/investigate/cyber/ncijtf (accessed 18 May 2013).

Table 1. Members of the National Cyber Investigative Joint Task Force

Members of the National Cyber Investigative Joint Task Force

Federal Bureau of Investigation	Defense Intelligence Agency
National Security Agency	National Geospatial Intelligence Agency
United States Secret Service	Defese Criminal Investigative Service
United States Department of Justice	United States Army 902d Military Intelligence Group
United States Department of Energy	United States Army Intelligence and Security Command
United States Department of State	United States Army Criminal Investigative Division
United States Department of Homeland Security	Naval Criminal Investigative Service
Central Intelligence Agency	United States Air Force Office of Special Invesigations
United States Department of Defense Cyber Crime Center	Joint Task Force - Global Network Operations

Source: U.S. Department of Justice, Audit report 11-22, "The Federal Bureau of Investigation's Ability to Address the National Security Cyber Intrusion Threat," April 2011, http://www.justice.gov/oig/reports/FBI/a1122r.pdf (accessed 7 May 2013).

The NCIJTF is comprised of key representation of 18 intelligence and law enforcement agencies. The task force is dedicated to operating as a joint and interagency force focused on collecting the intelligence necessary to predict and prevent future cyber attacks targeting the U.S. and critical national assets.

The NCIJTF does not concentrate on the reduction of cyber vulnerabilities throughout cyberspace. Despite NCIJTF's concentration solely on law enforcement actions to secure cyberspace, the task force embraces key and essential tenets of the President's CNCI, as well as Mission Command.

The NCIJTF structure supports a shared understanding and common operating picture in order to exploit the many jurisdictions, capabilities, and expertise throughout the 18 agencies and departments included within the task force. Additionally, the NCIJTF provides the means and medium necessary for effective collaboration, and certifies the agencies are operating within their legal means. Furthermore, the task force maximizes shared resources to target cyber threats, ultimately arrest cybercriminals, and protect global networks.

In conjunction with domestic efforts, the Federal Bureau of Investigation leads a strategic alliance with the Serious Organized Crime Agency (United Kingdom), Royal Canadian Mounted Police (Canada), Australian Federal Police (Australia), and New Zealand Police (New Zealand), as depicted in figure 5. The coalition of national law enforcement agencies provides the U.S. and partnered nations the ability to collaborate at a global in order to better protect the global information grid. Additionally with the complexity of combating cyber terrorists and criminals, the alliance creates task forces, as needed, to lead joint investigations that cross international borders and laws. The shared intelligence, collaboration of best practices and tools, combined with the establishment of working groups provide an international platform for strengthening and synchronizing laws and law enforcement techniques.[64]

[64]U.S. Department of Justice, "Cyber Solidarity: Five Nations, One Mission," Federal Bureau of Investigation, 18 March 2008, http://www.fbi.gov/news/stories/2008/march/cybergroup_031708 (accessed 18 May 2013).

Figure 5. Strategic Alliance Cyber Crime Working Group

Source: U.S. Department of Justice, "Cyber Solidarity: Five Nations, One Mission," Federal Bureau of Investigation, 18 March 2008, http://www.fbi.gov/news/stories/2008/march/cybergroup_031708 (accessed 18 May 2013).

Exercises

> Whoever can make and implement his decisions consistently faster gains a tremendous, often decisive advantage. Decision making thus becomes a time-competitive process, and timeliness of decisions becomes essential to generating tempo.[65]

Years of experience and growth facilitate a Commander's ability to proficiently blend the art and science of command. Experience built on a foundation of self-development, training, and education. Commanders will pull from their experiences in order to develop diverse live, constructive, and virtual training focused on cultivating leaders and increasing mission proficiency. Training exercises provide Commanders an

[65]U.S. Marine Corps, Fleet Marine Force Manual (FMFM) 1, *Warfighting* (Quantico, VA: Secretary of the Navy, 6 March 1989), 69.

opportunity to execute all key principles of Mission Command, while simultaneously developing their subordinate leaders.

Training exercises at each level, strategic, operational, and tactical, embody all six tenets to Mission Command. Strategic and operational level cyber exercises like Cyber Flag and Terminal Fury facilitate the building of joint and interagency teams through mutual trust. For instance, U.S. Pacific Command executes the activation of Joint Task Force 519 in support of their annual contingency response exercise, Terminal Fury. Despite not being a true standing task force, the Joint Task Force maintains its full capabilities to deploy in response to contingencies of small-scale operations up through to major theater conflict.[66] This unique nuance makes training the soldiers, sailors, marines, airmen, and interagency personnel who make up the headquarters an extreme challenge, especially as they come from all corners of the world. Through trust in the individuals and their parent commands and accepting prudent risk, the U.S. Pacific Command is confident the task force meets the bar for success, as evidenced in their annual capstone event, Terminal Fury.

In addition to building cohesive teams through trust, the U.S. Pacific Command Commander provides clear intent of training expectations through mission orders and a rigorous annual training plan. U.S. Pacific Command and Joint Task Force 519 utilize interactive websites in order to facilitate the training of the staff and, thus, ensuring fully

[66]Walter F. Doran, "Pacific Fleet Focuses on War Fighting," *Proceedings* 129, no. 8 (August 2003): 58, http://web.ebscohost.com.lumen.cgsccarl.com/ehost/detail?vid=5&sid=e37c0273-c8b1-4995-80cb-f06ec93221c9%40sessionmgr12&hid=20&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=mth&AN=10494781 (accessed 20 May 2013).

trained leaders. Furthermore, the websites support collaborative training and interactive problem solving for the staff regardless of geographical location.[67]

While Joint Task Force 519 and Terminal Fury focuses on the Pacific area of responsibility, Cyber Flag is a critical exercise, led by USCYBERCOM, for the DoD in order to train their cyber leaders and build upon the capabilities of their subordinate commands. The Cyber Flag 12-1 exercise took place in November 2011 on a private virtual network in order to train and increase our cyber warriors' technical capacity and capability. Exercise participants included approximately 300 of the DoD's best cyber warriors, uniformed and civilian. The focus was to exercise both our offensive and defensive cyber tactics, while capitalizing on an opportunity to exercise a joint sub-unified command.

As USCYBERCOM continued to evolve their exercise and leader development program, Cyber Flag 13-1 expanded its scope and exercise objectives through increasing the training audience to approximately 700 personnel, more than doubling the virtual network, and included other government partners. The second annual Cyber Flag exercise concentrated on the nesting the service component cyber organizations, like Army Cyber Command, personnel and missions with that of USCYBERCOM, while integrating other cyber and network defense organizations, such as the Defense Information Systems Agency.[68] "The inclusion of several operational elements this year [Cyber Flag 13-1]

---

[67]Doran, 58.

[68]"Annual US Cyber Flag Exercise Provides Realistic Training," *Cyber Defense Magazine*, http://www.cyberdefensemagazine.com/annual-us-cyber-flag-exercise-provides-realistic-training/#sthash.Ti2KQE4T.QRvmwZeZ.dpbs (accessed 21 May 2013).

reinforced a warrior mind-set, which helps us to succeed in this domain in the defense of our nation."[69]

Lastly, cyber exercises like Terminal Fury and Cyber Flag provide a medium for leaders at all levels to exercise disciplined initiative, while minimizing collateral damage to live networks. Exercise designs implement control measures while maintaining the integrity of the exercise and ensuring training objectives are met. Thus providing commanders the ability for input on the acceptance of risk for resources (time, people, and money), potential loss of productivity, and competing mission's success.[70]

Education

Leadership and learning are indispensable to each other.[71]

Along with standard military education requirements, cyber soldiers and leaders are required to see self-development and continue education in the field of cyber and information technology. Additionally, President Barack Obama highlighted the importance of continued education of our cyber experts as part of the CNCI #8,

> while billions of dollars are being spent on new technologies to secure the U.S. Government in cyberspace, it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success. However there are not enough cybersecurity experts within the Federal Government or private sector to implement the CNCI, nor is there an adequately established Federal cybersecurity career field. Existing cybersecurity training and personnel development programs, while good, are limited in focus and lack unity of effort. In order to effectively ensure our continued technical advantage and future cybersecurity, we must develop a technologically-skilled and cyber-savvy

[69]"Annual US Cyber Flag Exercise Provides Realistic Training."

[70]LTC Frank J. Snyder, "Incorporating Cyber in Exercises."

[71]BrainyQuote, "John F. Kennedy Quotes," http://www.brainy quote.com/quotes/quotes/j/johnfkenn130752.html (accessed 4 June 2013).

> workforce and an effective pipeline of future employees. It will take a national strategy, similar to the effort to upgrade science and mathematics education in the 1950s, to meet this challenge.[72]

Despite challenges to train and maintain proficient and professional IT specialists, the DoD and the Army have implemented several programs to better educate and develop cyber soldiers and leaders. Programs like Training with Industry (TWI), cyber and IT degree opportunities, and the DoD Information Assurance Workforce Improvement Program are just a few of the methods the Army utilizes to educate their cyber leaders.

TWI provides young leaders (officers, warrant officers, and non-commissioned officers) the opportunity to immerse themselves into the private sector, cyber and communications industry. Additionally, TWI allows the Army to develop leaders with business and technical skills that are otherwise not available through standard Army training centers. Following their assignment with industry, these leaders are then matched into positions within the Army that best optimize the knowledge and training received in order to inculcate lessons learned into the culture of cyber leaders. Table 2 is the most recent list of TWI corporations the Army has agreements with to train its leaders.

[72]The White House, "The Comprehensive National Cybersecurity Initiative."

Table 2. Training with Industry Opportunities

Officer	
Signal (25)	Lockheed Martin Information Sys & Global Svc
	General Dynamics
	Lincoln Laboratory
Telecommunication Systems Engineering (FA24)	CISCO Systems Inc.
	Northrup Grumman Corp
	McAfee Inc.
Information Systems Management (FA53)	Google Inc.
	Microsoft Corp
	Raytheon Cyber Security Solutions
	AT&T Corp
Warrant Officer	
Signal (25)	CISCO Systems, Inc.
	General Dynamics
	Microsoft Corp
	Intelsat
Non-Commission Officer	
Signal (25)	CISCO Systems Inc.

Source: U.S. Army Resources Command, "Training with Industry Opportunities," https://www.hrc.army.mil/Officer/Training%20With%20Industry%20TWI%20List%20of%20Companies (accessed 24 May 2013).

Programs like TWI, assure trust in the commercial industry and their ability to train and develop Army leaders to combat the enemy in cyberspace. Additionally, TWI builds on the relationships between private business and the government to ensure the successful defense of the nation. Despite the challenges to train and maintain IT personnel, the DoD and the Army have implemented several programs to better educate and develop cyber soldiers and leaders.

In order to further combat the shortage of trained and educated cyber/information technology specialists, each of the service academies have implemented degree programs for their cadets in such areas of emphasis. For example, the Air Force Academy has offered cadets a degree in computer science-cyberwarfare (originally called computer science-information assurance) since 2004. The courses within the curriculum include cryptology, information warfare and network security. As a result, 25 cadets from the Air Force Academy will graduate in 2013 with a computer science-cyberwarfare degree, and they will go on to be assigned to USCYBERCOM.[73]

In 2005, the DoD implemented the 8570.01-M, *Information Assurance Workforce Improvement Program*, as the guiding manual for the management of IA personnel, along with establishing a common baseline of training requirements for all DoD personnel. [74] While outlining requirements, it represents the dependence of the DoD on the IT industry standard certifications and training programs in order to properly and sufficiently educate their personnel. Figure 6 outlines the list of certifications required by IA workforce category and level of responsibility. As an example, many IT specialists at the strategic and operational levels typically meet the requirements within the Information Assurance Management or Information Assurance System Architect and Engineer categories. While the training is invaluable, constant recertification adds to the challenges for leaders.

[73]Associated Press, "Military Grooming New Officers for War in Cyberspace," *Fox News*, 26 April 2013, http://www.foxnews.com/us/2013/04/26/military-grooming-new-officers-for-war-in-cyberspace/?test=latestnews#ixzz2UKlNHaM9 (accessed 18 May 2013).

[74]Department of Defense, Department of Defense 8570.01-M, 12.

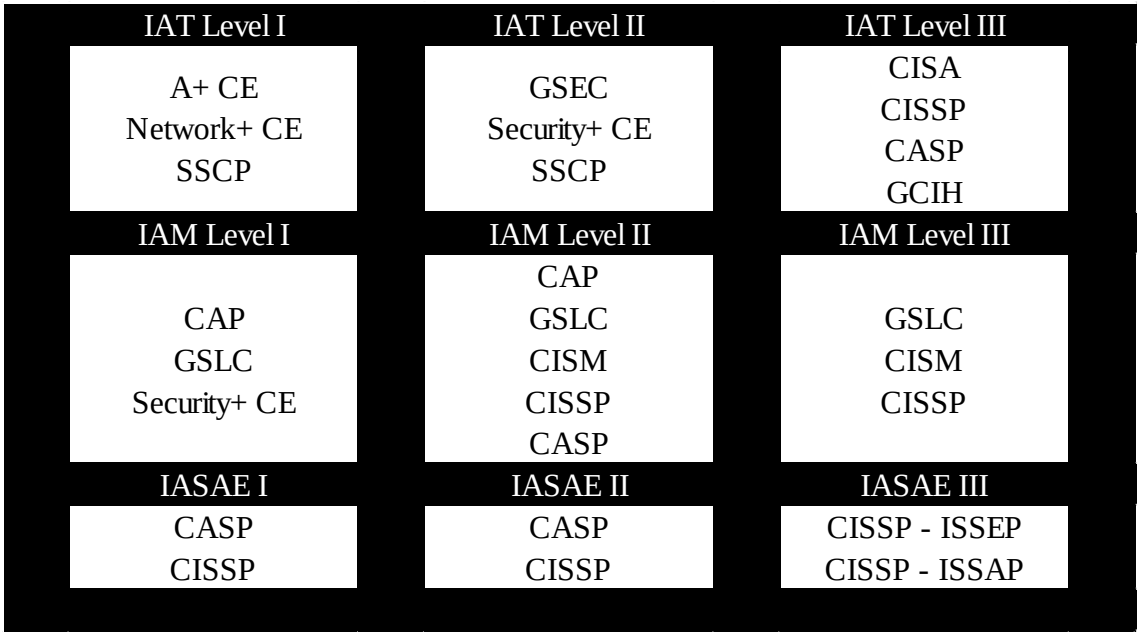


Figure 6. DoD Approved Baseline Certifications

Source: Information Assurance Support Environment, "DoD Approved Baseline Certifications," Defense Information Systems Agency, http://iase.disa.mil/eta/iawip/content_pages/iabaseline.html (accessed 24 May 2013).

Summary to Primary Research Question

The interdependence of Mission Command and leader development of cyber warriors is critical throughout the cyber organizations. The DoD command structure relies on a unified command strategy, clear commander's intent, mutual trust, collaboration throughout the DoD and its partner agencies in order to properly secure the cyber domain. The research also shows the dependence on educational programs, such as TWI and certifications. The relationships between private business and the government to ensure the successful development of cyber leaders are imperative to the success of developing technically and tactically proficient cyber leaders. Lastly, joint and national level cyber exercises provide a media for leaders to exercise disciplined initiative,

develop mission orders, accept risk, set a clear commander's intent, establish a common operating picture, and build teams, relationships, and trust.

Answers to Secondary Research Questions

The secondary research questions presented earlier were:

1. In applying economy of force, are there areas of expertise and resources in the Joint, Inter-Agency, or commercial environments the Army can and should rely on to develop its cyber soldiers and leaders?
2. Can a Joint and/or "Whole of Government" approach in the development of future cyber leaders?
3. How can the current Army and Cyber/Communications culture benefit from embracing General Dempsey's tenant of "trust" in the future operations?"

The next segment of this thesis will answer those questions.

Question 1

The research showed several areas of expertise the Army can rely on to assist in the development of cyber leaders and soldiers. First and foremost, the DoD must continue to rely on commercial IT certifications and higher education to further educate and develop cyber leaders. Universities and the IT industry possess the expertise to train and educate on cyber that cannot otherwise be replicated within the Army, either due to cost or availability.

Secondly, agencies, such as the Federal Bureau of Investigation, possess the criminal investigations and cyber forensics experts. Although focused on law enforcement, the experts operating in the law enforcement Title 18 role can assist in

reverse engineering cyber attacks in order to facilitate building necessary parameters to prevent future similar attacks against U.S. valued interests. Organizations like the NCIJTF, provide leaders assigned to the 902d Military Intelligence Group, Intelligence and Security Command, and Criminal Investigative Division the exposure to collaborative forums of cyber expertise, such as the NCIJTF.

Due to the complexity, intense resources, and expertise required to execute cyber exercises, joint and interagency exercises – such as Terminal Fury and Cyber Flag– provide the Army the training environment to further develop cyber leaders who may otherwise be passed up in today's resource-constrained environment.

Question 2

The research showed that joint and the whole of government approach could assist in the development of cyber leaders, though primarily at the flag command level. Organizations like USCYBERCOM headquarters, NCIJTF, NCCIC, and Joint Task Force 519 headquarters have set conditions for collaboration and a shared understanding of the current state of cyber operations, as well as the development and improvement of techniques, tactics, and procedures for cyber operations. These conditions facilitate a positive culture and climate for the development, coaching, and mentorship of the cyber leaders assigned. The research also showed these elements and headquarters facilitate ongoing development.

Question 3

> A learning organization is an organization skilled at creating, acquiring, interpreting, transferring, and retaining knowledge, and at purposefully modifying its behavior to reflect new knowledge and insight.[75]

Trust is a critical foundation of every learning organization. Within the cyber domain, organizations have a greater trust in the adjacent units and agencies in order to effectively defend the network and cyberspace. Additionally, the culture and climate of cyber organizations must have trust in the federal government, policy, and strategy.

The defense of cyberspace demands an organization's culture and climate have a foundation of trust to effectively operate and defend the network. While the individual services and agencies own and operate their networks, a culture of trust is essential in for further collaboration and sharing of lessons learned. The culture of cyber leaders and organizations must move past simply observing lessons through exercise and training after actions reviews, but focus on truly learning lessons and indoctrinate them into the organization's culture. Additionally, the sharing of lessons learned with all cyber organizations not only assists in developing leaders, but also builds trust throughout the organizations, military and civilian alike. Lastly, "the number of 10-pound brains in any nation is limited,"[76] and the cyber culture must establish the culture to best utilize the cyber experts throughout the government.

---

[75]David A. Garvin, *Learning in Action* (Boston, MA: Harvard Business Review Press, 2000), 11.

[76]Stew Magnuson, "When it Comes to Cybersecurity, the 'Who is Responsible for What?' Debate Continues," *National Defense*, June 2011, http://www.nationaldefense magazine.org/archive/2011/June/Pages/WhoisResponsibleforCybersecurity.aspx (accessed 12 May 2013).

Summary

The demands of cyberspace require a cyber leader to be agile, adaptive, and technically and tactically proficient in defending the network. However, the direct correlation between Mission Command and cyber leader development was unable to be conclusive due to the number of variables. However, the research proved the six elements of Mission Command are indirectly guiding the potential development of cyber leaders.

Building Cohesive Teams through Mutual Trust

The cyber community established coordination centers and headquarters with the intent of building cohesive teams and fostering a climate of mutual trust. For example, the NCCIC and NCIJTF coordinate with federal agencies and departments, as well as the occasional civilian organization, in order to secure the government's cyber operating environment. Additionally, Joint Task Force 519 is built around a joint and interagency structure that trains throughout the year in order to build a singular team from personnel who have daily responsibilities to their parent service or agency. Furthermore, relationships between private business and the government built on programs like TWI and IT industry standard certifications and training ensure the successful development of technical cyber leaders.

Lastly, the current cyber organizational structure supports the establishment of a culture and climate inviting to the building of cohesive teams through mutual trust.

Create Shared Understanding

The second tenet of Mission Command is fostered through command relationships and the direct interaction of key organizations. The NCCIC, NCIJTF,

Strategic Alliance Cyber Crime Working Group, and Joint Task Force-519 were each established to share intelligence, collaborate on their best practices and tools, and synchronize tactics, techniques, and procedures. Additionally, the baseline training standards established by DoD 8570.01-M institute a common understanding, expectations, and education of cyber warriors across DoD cyber formations.

Clear Commander's Intent and Use Mission Orders

USCYBERCOM enables the propagation of the Commander's intent primarily through the command relationships within the DoD. With General Keith Alexander dual-hatted as the Commander of USCYBERCOM and Director of the National Security Administration, the DoD command structure for cyber operations supports a unified command strategy, promotes a clear commander's intent, and enables nesting of the DoD cyber mission with the National Command Authority's strategy. Since USCYBERCOM does not have any cyber formations under their direct command, Cyber Command utilizes an operational control relationship with the service components cyber formations in order to ensure a clear intent throughout the DoD. Additionally, Cyber Flag and Terminal Fury exercises have allowed strategic cyber commanders the ability to validate their mission, vision, and intent through mission orders.

Exercise Disciplined Initiative

Cyber exercises like Terminal Fury and Cyber Flag provide a medium for leaders at all levels to exercise disciplined initiative. Thus, recent exercises have been designed to allow for cyber leaders to apply disciplined initiative, while simultaneously

implementing control measures to ensure training objectives are met and minimal risk of collateral damage to live networks.

Accept Prudent Risk

Exercise designs implement control measures while maintaining the integrity of the exercise and ensuring training objectives are met. Thus, effectively designed exercises provide commanders the ability for input on the acceptance of risk for resources (time, people, and money), potential loss of productivity, and competing mission's success.[77] Additionally, the Army must take prudent risk in the placement of its leaders. While placing the right person in the right job at the right time, leaders must accept risk at times in order to ensure the greater good of all cyber organizations. Although broadening is essential for leader development, the propagation of the expert's knowledge to the rest of the force must be sufficiently weighed out as well. Lastly, the DoD has accepted a level of risk in the organizational structure of USCYBERCOM, through allowing just operational control of DoD cyber formations. Thus, USCYBERCOM is left with just the staff to coordinate with the individual service's cyber units in order to execute cyber directives.

This chapter was divided into two sections. The first section of the chapter addressed the analysis of mission command and leadership as it applied to operational and strategic level organization, exercises, and education/training. The second section of this chapter revisited the research data in order to address the secondary questions, and support the proposed recommendations in the next chapter.

[77]Snyder, 10.

CHAPTER 5

RECOMMENDATIONS

> Signal is a combat arm, and information is an element of combat power.[78]
> — Lieutenant General B. B. Bell, III, quoted in Via and Jantzen, "Bridging the 'Digital Delta': Training III Corps Signaleers"

Mission Command is not simply a philosophy or warfighting function, but a potential method and guideline for the development of soldiers and civilians throughout the DoD and the IT industry. The research demonstrates that the Army should continue to embrace and broaden the TWI programs. The increased partnerships need to be specific to cyberspace and computer network operations in order to expand the expertise residing within the DoD, the Army, and the civilian sector.

Despite being at the risk to the active duty workforce, a prudent risk for the long-term success of leaders would be to provide more openings for TWI, assignments to joint cyber organizations, and other education opportunities. The accepted risk and additional development opportunities should increase the overall competency of the Army's cyber defense.

Culture and climate are essential to establishing a learning organization. Trust as part of the culture and climate is critical in building the foundation of an organization. Trust occurs at every level; from the leaders, soldiers, civilians and the higher headquarters. Trust should be established within the subordinate units to accomplish their assigned mission and responsibilities.

---

[78]LTG B. B. Bell, III, quoted in Via and Jantzen, "Bridging the 'Digital Delta': Training III Corps Signaleers," 40.

Within the cyber domain, trust can become a type of currency, whereby organizations who have established reliance and trust, would be able to effectively exchange concepts and ideas to help defend their respective area of responsibility within the greater common of cyberspace.

Additionally, the Army must assume prudent risk in the placement of its leaders within key cyber organizations. While maximizing a leader's expertise – the right person for the right job at the right time – is critical to ensuring effective organizations are adequately staffed. The broadening of cyber warriors is essential for well-rounded leader development. The expert's knowledge and experiences are essential to propagate across the rest of the force.

Finally, the defense of cyberspace should be a global mission. The national strategy should include the United Nations for international policy, and establish actionable legislation defining the parameters for operating within cyberspace. In conjunction with representatives of the DoD, Department of Justice, and Department of Homeland Security, the Department of State should lead an international working group, with our Five Eyes partnership and the United Nations, in order to establish international standards of conduct for sharing a cyberspace which is truly a global common.

Future Research

To better define and understand the future of cyberspace and how the nation can best combat the growing threats within the cyber domain, the following topics should be researched:

1. Would a single joint organization from top to bottom under Cyber Command improve the DoD's posture for computer network operations;

2. Can a Single Cyber Center of Excellence be established to train all cyber leaders, soldiers, sailors, airmen, and marines in order to maximize training quality while minimizing cost and resources;
3. Lastly, can all Sister Services benefit from adopting Mission Command into their doctrine?

Summary

As the U.S. government continues to define and function in the complex operating environment of cyberspace, commanders and leaders at all levels must develop dynamic, malleable, and knowledgeable leaders and soldiers to combat the emerging cyber threats. Commanders will need to establish learning environments and opportunities that allow for discipline initiative, while accepting there will be the occasional failures. In return, leaders must establish a culture and climate within the organization that fosters prudent risk, while ensuring failure is survivable–a safe fail. Lastly, commanders and organizations must learn from their failures. Many times, leaders and organizations observe lessons, though fail to inculcate them into the organization's culture to truly learn from the failures. While a cyber warrior must be technically and tactically proficient in the cyber domain, it is just as critical that he/she be a better leader in the asymmetric dynamics of cyberspace. The demands of cyberspace, evolution, progression, and continued ambiguity of the environment require leaders who are agile, adaptive, and aggressive.

There is a direct correlation between Mission Command and the development of current and future cyber warriors throughout all formations, organizations, and agencies

within the U.S. While a single agency cannot protect and defend cyberspace alone, the government and private sector, collectively, can effectively defend the nation's assets.

The Army must take prudent risk in the placement of its leaders within key cyber organizations. While maximizing a leader's expertise–right person for the right job at the right time–is critical to ensuring effective organizations, broadening is essential for leader development, as well as the propagation of the expert's knowledge to the rest of the force.

BIBLIOGRAPHY

Government Documents

Chairman of the Joint Chiefs of Staff. Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms.* Washington, DC: Government Printing Office, 8 November 2010, as amended through 15 July 2011.

Headquarters, Department of the Army. Army Doctrine Reference Publication (ADRP) 1-02, Change 2, *Operational Terms and Military Symbols.* Washington, DC: Government Printing Office, 28 November 2012.

_____. Army Docrine Reference Publication (ADRP 6-0), *Mission Command.* Washington, DC: Government Printing Office, 17 May 2012.

_____. Army Doctrine Reference Publication (ADRP) 6-22, Change 1, *Army Leadership.* Washington, DC: Government Printing Office, 10 September 2012.

_____. Department of the Army Pamphlet (DA PAM) 350-8, *Army Leader Development Program.* Washington, DC: Government Printing Office, 8 March 2013.

_____. TRADOC Pamphlet 525-7-8, *Cyberspace Operations Concept Capability Plan 2016-2028*. Fort Monroe, VA: Training and Doctrine Command, 22 February 2010.

U.S. Air Force. Air Force Doctrine Document (AFDD) 2-8, *Command and Control.* Washington, DC: Air Force Departmental Publishing Office, 1 June 2007.

U.S. Congress. Senate Armed Services Committee. "Statement of Secretary of the Army John M. McHugh and General Raymond T. Odierno." 113th Cong., 1st sess., 23 April 2013.

U.S. Marine Corps. Fleet Marine Force Manual (FMFM) 1, *Warfighting.* Quantico, VA: Secretary of the Navy, 6 March 1989.

_____. Marine Corps Doctrinal Publication (MCDP) 6, *Command and Control.* Quantico, VA: Secretary of the Navy, 4 October 1996.

Internet Sources

24th Air Force. "24th Air Force Fact Sheet." 3 January 2013. http://www.24af.af.mil/library/factsheets/factsheet.asp?id=15663 (accessed 3 April 2013).

Alexander, Keith B. “Warfighting in Cyberspace.” *Joint Forces Quarterly*, no. 46 (3d Quarter 2007): 59. http://www.carlisle.army.mil/DIME/documents/Alexander.pdf (accessed 5 June 2013).

_____. Quoted in Cheryl Pellerin. “Cybersecurity Involves Federal, Industry Partners, Allies.” *American Forces Press Service*, 8 November 2012. http://www.defense.gov/news/newsarticle.aspx?id=118479 (accessed 16 February 2013).

“Annual US Cyber Flag Exercise Provides Realistic Training.” *Cyber Defense Magazine*. http://www.cyberdefensemagazine.com/annual-us-cyber-flag-exercise-provides-realistic-training/#sthash.Ti2KQE4T.QRvmwZeZ.dpbs (accessed 21 May 2013).

Associated Press. “Military Grooming New Officers for War in Cyberspace.” *Fox News*, 26 April 2013. http://www.foxnews.com/us/2013/04/26/military-grooming-new-officers-for-war-in-cyberspace/?test=latestnews#ixzz2UKlNHaM9 (accessed 18 May 2013).

Bajaj, Kamlesh. “Cyberspace as Global Commons.” *Dataquest.* General OneFile, 14 May 2012. http://go.galegroup.com.lumen.cgsccarl.com/ps/i.do?id=GALE%7CA289665832&v=2.1&u=97mwrlib&it=r&p=ITOF&sw=w (accessed 5 June 2013).

Blank, Steve. “Flying High: Why The Military Is Taking Cyber Warfare Seriously.” *Forbes*, 29 April 2013. http://www.forbes.com/sites/steveblank/2013/04/29/fly-high-cyber-warfare-military/ (accessed 25 May 2013).

Bowden, Mark. “The ‘Worm’ That Could Bring Down The Internet.” NPR Books, 27 September 2011. http://www.npr.org/2011/09/27/140704494/the-worm-that-could-bring-down-the-internet (accessed 29 May 2013).

BrainyQuote. “John F. Kennedy Quotes.” http://www.brainyquote.com/quotes/quotes/j/johnfkenn130752.html (accessed 4 June 2013).

Caslen, LTG Robert L. Jr., and Colonel(Promotable) Charles A. Flynn. “Introducing the Mission Command Center of Excellence.” *Army* 61, no. 2 (February 2011): 53-56. http://www.ausa.org/publications/armymagazine/archive/2011/2/Documents/Caslen_Flynn_0211.pdf (accessed 24 September 2012).

Corrin, Amber. “Service Academies Ramp Up Cyber Training.” *Business of Federal Technology*, 26 April 2013. http://fcw.com/articles/2013/04/26/cyber-training-academy.aspx (accessed 25 May 2013).

Davidson, Don. *Comprehensive National Cyber Security Initiative (CNCI) & ICT Supply Chain Risk Management (SCRM).* National Defense Industrial Association Logistics, 16 October 2009. http://www.ndia.org/Divisions/Divisions/Logistics/Documents/DD%20at%20NDIA%20Log%2016oct.pdf (accessed 10 May 2013).

Dempsey, Martin. *Mission Command White Paper*. Joint Chiefs of Staff, 3 April 2012. http://www.jcs.mil/content/files/2012-04/042312114128_CJCS_Mission_Command_White_Paper_2012_a.pdf (accessed 24 May 2013).

Department of Defense. Department of Defense 8570.01-M, *Information Assurance Workforce Improvement Program.* Incorporating Change 3, 24 January 2012. http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf (accessed 14 May 2013).

_____. *The Strategy for Homeland Defense and Civil Support.* Washington, DC: Government Printing Office, June 2005.

_____. *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense.* January 2013. http://iase.disa.mil/policy-guidance/dasd_ciia__strategy_aug2009.pdf (accessed 12 May 2013).

Department of Homeland Security. *National Cyber Incident Response Plan*, Interim Version, September 2010. http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf (accessed 18 May 2013).

Doran, Walter F. "Pacific Fleet Focuses on War Fighting." *Proceedings* 129, no. 8 (August 2003): 58, http://web.ebscohost.com.lumen.cgsccarl.com/ehost/detail?vid=5&sid=e37c0273-c8b1-4995-80cb-f06ec93221c9%40sessionmgr12&hid=20&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=mth&AN=10494781 (accessed 20 May 2013).

Edwards, David. "Cadets Study Art of Cyber Warfare." The Official Web Site of the U.S. Air Force, 22 July 2011. http://www.af.mil/news/story.asp?id=123265104. (accessed 25 May 2013).

Garamone, Jim. "Lynn Notes Cyber Command's Significance." *American Forces Press Service*, 21 May 2010. http://www.defense.gov/news/newsarticle.aspx?id=59295 (accessed 2 May 2013).

Holstead, LT Joseph. "US Tenth Fleet Cyber Warriors Support Exercise CYBER FLAG 13-1." Defense Video and Imagery Distribution System, 20 November 2012. http://www.dvidshub.net/news/98136/us-tenth-fleet-cyber-warriors-support-exercise-cyber-flag-13-1#.UZ2VJLXvtL9 (accessed 20 May 2013).

IBLS Editor. "Internet Law-New US National Cyber Investigative Joint Task Force Will Be Led by FBI." Internet Business Law Services. http://www.ibls.com/internet_law_news_portal_view.aspx?id=2044&s=latestnews (accessed 17 May 2013).

Information Assurance Support Environment. "DoD Approved Baseline Certifications." http://iase.disa.mil/eta/iawip/content_pages/iabaseline.html (accessed 24 May 2013).

International Air Transport Association. “The Early Days.” http://www.iata.org/about/Pages/history_2.aspx (accessed 1 May 2013).

Jabbour, Dr. Kamal T. “50 Cyber Questions Every Airman Can Answer.” Air ForceResearch Laboratory, 7 May 2008. http://www.au.af.mil/au/awc/awcgate/afrl/50_cyber_questions.pdf (accessed 20 May 2013).

Juhl, Felix, and Heiko Borchert. “Exploiting the Potential of Cyber Operations.” *Jane’s Defence Weekly* 48, no. 26 (29 June 2011). https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=News&ItemId=+++1187350&Pubabbrev=JDW (accessed 19 February 2013).

Leiter, Michael. “Analysis: As Cyberthreat Looms, Here's What Really Matters.” NBCNews.com, 22 February 2013. http://usnews.nbcnews.com/_news/2013/02/22/17057322-analysis-as-cyberthreat-looms-heres-what-really-matters?lite (accessed 24 February 2013).

Magnuson, Stew. “When it Comes to Cybersecurity, the ‘Who is Responsible for What?’ Debate Continues.” *National Defense*, June 2011. http://www.nationaldefensemagazine.org/archive/2011/June/Pages/WhoisResponsibleforCybersecurity.aspx (accessed 12 May 2013).

Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer. *Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance Strategy*, August 2009. http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf (accessed 14 May 2013).

Oxford Dictionaries. “Global Commons.” http://oxforddictionaries.com/us/definition/american_english/global%2Bcommons (accessed 17 March 2013).

Pellerin, Cheryl. “Cybersecurity Involves Federal, Industry Partners, Allies.” *American Forces Press Service*, 8 November 2012. http://www.defense.gov/news/newsarticle.aspx?id=118479 (accessed 16 February 2013).

Ramsey, LTC Marshall N. “Training With Industry.” *Army Sustainment* 42, no. 3 (May/June 2010): 50-51. http://www.almc.army.mil/alog/issues/May-June10/train_windustry.html (accessed 18 May 2013).

Reimer, Jordan. “U.S. Cyber Command Preparations Under Way, General Says.” *American Forces Press Service*, 17 March 2010. http://www.af.mil/news/story.asp?id=123195306 (accessed 16 February 2013).

Secretary of Defense. Memorandum, “Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations,” 23 June 2009. http://www.defense.gov/home/features/2010/

0410_cybersec/docs/cyber_command_gates_memo[1].pdf (accessed 1 October 2012).

U.S. Air Force. “U.S. Air Force Mission Statement.” http://www.af.mil/main/welcome.asp (accessed 24 October 2012).

U.S. Army Cyber Command/U.S. 2d Army. “United States Cyber Command Mission.” http://www.arcyber.army.mil/org-uscc.html (accessed 14 October 2012).

U.S. Army Human Resources Command. “Training with Industry Opportunities.” https://www.hrc.army.mil/Officer/Training%20With%20Industry%20TWI%20List%20of%20Companies (accessed 24 May 2013).

U.S. Army Network Enterprise Technology Command. “NETCOM Mission and Vision.” http://www.army.mil/info/organization/unitsandcommands/commandstructure/netcom/ (accessed 14 October 2012).

U.S. Congress. House. “Statement of Major General Rhett Hernandez, USA, Incoming Commanding General, U.S. Army Forces Cyber Command before the House Armed Services Committee, Subcommittee on Terrorism, Unconventional Threats and Capabilities.” 111th Cong., 2nd sess., 23 September 2010. http://democrats.armedservices.house.gov/index.cfm/files/serve?File_id=067ffc96-e5c1-4cef-baa2-010d16e3be57 (accessed 24 September 2012).

U.S. Department of Defense. *National Defense Strategy*. June 2008. http://www.defense.gov/news/2008%20National%20Defense%20Strategy.pdf (accessed 4 June 2013).

U.S. Department of Homeland Security. “About the National Cybersecurity and Communications Integration Center.” http://www.dhs.gov/about-national-cybersecurity-communications-integration-center (accessed 22 May 2013).

U.S. Department of Justice., Audit Report 11-22, “The Federal Bureau of Investigation’s Ability to Address the National Security Cyber Intrusion Threat.” April 2011. http://www.justice.gov/oig/reports/FBI/a1122r.pdf (accessed 7 May 2013).

_____. “Cyber Solidarity: Five Nations, One Mission.” Federal Bureau of Investigation. 18 March 2008. http://www.fbi.gov/news/stories/2008/march/cybergroup_031708 (accessed 18 May 2013).

_____. “National Cyber Investigative Joint Task Force.” Federal Bureau of Investigation. http://www.fbi.gov/about-us/investigate/cyber/ncijtf (accessed 18 May 2013).

U.S. Fleet Cyber Command, U.S. 10th Fleet. “U.S. Fleet Cyber Command Mission and U.S. Tenth Fleet Mission.” http://www.fcc.navy.mil/ (accessed 14 October 2012).

U.S. Government Accountability Office. “Military Transformation: Additional Actions Needed by U.S. Strategic Command to Strengthen Implementation of Its Many Missions and New Organization.” September 2006. http://www.gao.gov/new.items/d06847.pdf (accessed 2 May 2013).

United Nations. *United Nations Treaties and Principles On Outer Space, related General Assembly, resolutions and other documents.* http://www.unoosa.org/pdf/publications/st_space_61E.pdf (accessed 1 May 2013).

Van Houten, Vincent. “An Overview of the Cyber Warfare, Exploitation & Information Dominance (CWEID) Lab.” Systems Center Atlantic, 28 January 2010. http://info.publicintelligence.net/cyberwarfarebrief.pdf (accessed 17 May 2013).

Vitas, Michael. “The Next Battlefield: The Reality of Virtual Threats.” *Global Catastrophe* 28, no. 3 (Fall 2006): 3-6. http://www.nyu.edu/intercep/lapietra/Vatis_TheNextBattlefieldTheRealityofVirtualThreats.pdf (accessed 20 October 2012).

Watson, Stephen. “Training Cyber Defenders.” America’s Intelligence Wire, 28 October 2012. http://go.galegroup.com.lumen.cgsccarl.com/ps/i.do?id=GALE%7CA306738033&v=2.1&u=97mwrlib&it=r&p=ITOF&sw=w (accessed 24 May 2013).

The White House. “The Comprehensive National Cybersecurity Initiative.” National Security Council, 19 February 2013. http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (accessed 20 October 2012).

Other Sources

Bell, Lieutenant General B. B. III. Quoted in Colonel Dennis Via and Major Linda Jantzen. “Bridging the ‘Digital Delta’: Training III Corps Signaleers.” *Army Communicator* 27, no. 2 (Summer 2002): 44.

Garvin, David A. *Learning in Action.* Boston, MA: Harvard Business Review Press, 2000.

Hansen, Major Andrew P., USAF. “Cyber Flag: A Realistic Cyberspace Training Construct.” Air Force Institute of Technology, Wright Patterson Air Force Base, OH, March 2008.

Snyder, LTC Frank J. Slide Presentation, “Incorporating Cyber in Exercises.” U.S. Pacific Command, 15 August 2012.

Van Creveld, Martin. *Command in War*. Quoted in U.S. Marine Corps. Marine Corps Doctrine Publication (MCDP) 6, *Command and Control.* Washington, DC: Government Printing Office, 4 October 1996.

_____. Quoted in LTC Frank J. Snyder. Slide Presentation, “Incorporating Cyber in Exercises.” U.S. Pacific Command, 15 August 2012.

Via, Colonel Dennis, and Major Linda Jantzen. “Bridging the ‘Digital Delta’: Training III Corps Signaleers.” *Army Communicator* 27, no. 2 (Summer 2002): 44.